COMMENTARII MATHEMATICI
UNIVERSITATIS SANCTI PAULI
Vol. 52, No. 1 2003

ed. RIKKYO UNIV/MATH
IKEBUKURO TOKYO
171–8501 JAPAN

Note on the Ring of Integers of a Kummer Extension of Prime Degree, I

by

Humio ICHIMURA

(Received October 21, 2002)
(Revised February 10, 2003)

Abstract. Let p be a prime number, and K a number field with $\zeta_p \in K^\times$. Let a be an integer of K relatively prime to p such that the principal ideal $a\mathcal{O}_K$ is square free in the semi-group of integral ideals of K. We prove that the Kummer extension $K(a^{1/p})/K$ has a power integral basis if it has a normal integral basis. Further, we show some related topics.

1. Introduction

Let L/K be a finite extension of a number field K, and $\mathcal{O}_K$ (resp. $\mathcal{O}_L$) the ring of integers of K (resp. L). The extension has a power integral basis (PIB for short) when $\mathcal{O}_L = \mathcal{O}_K[\gamma]$ for some $\gamma \in \mathcal{O}_L$. If L/K is Galois with group G, it has a normal integral basis (NIB for short) when $\mathcal{O}_L$ is free (of rank one) over the group ring $\mathcal{O}_K[G]$. Let p be a fixed prime number, and L/K a Kummer extension of degree p. When L/K is unramified (at all finite prime divisors), it is known by Childs [1, Theorem B] that L/K has a PIB if it has a NIB. For this, see also [6]. The main purpose of this note is to generalize this assertion for a certain tamely ramified case. We say that an integral ideal $\mathfrak{A}$ of $\mathcal{O}_K$ is square free (at K) when $\mathfrak{p}^2 \nmid \mathfrak{A}$ for all prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$. We show the following:

THEOREM 1. (I) *Let $p \geq 3$, and K a number field containing a primitive p-th root ζ_p of unity. Let a be an integer of K relatively prime to p such that the principal integral ideal $a\mathcal{O}_K$ is square free. Then, the Kummer extension $K(a^{1/p})/K$ has a PIB if it has a NIB.*

(II) *Let $p = 2$. A quadratic extension L/K of a number field K has a PIB if it has a NIB.*

The converse of Theorem 1 does not hold in general. Actually, we can show the following:

PROPOSITION 1. *Let $p \geq 3$. For any multiple N of $2(p-1)$, there exist infinitely many couples $(K, [a])$ of a CM-field K and a class $[a]$ in $K^\times/(K^\times)^p$ containing an integer a of K relatively prime to p such that* (i) $\zeta_p \in K^\times$ *and* $[K : \boldsymbol{Q}] = N$, (ii) *the integral ideal*

$a\mathcal{O}_K$ is square free, and (iii) *the Kummer extension $K(a^{1/p})/K$ is at most tamely ramified and has a PIB but no NIB.*

In Theorem 1 (I), we can not remove the condition that $a\mathcal{O}_K$ is square free because of the following assertion.

PROPOSITION 2. *Let p and K be as in Theorem* 1 (I). *There exist infinitely many Kummer extensions $L = K(a^{1/p})/K$ with a an integer of K relatively prime to p such that* (i) *$a\mathcal{O}_K$ is not square free and* (ii) *L/K has a NIB but no PIB.*

REMARK 1. (I) The second assertion of Theorem 1 is already given in Srivastav and Venkataraman [10, Theorem 2]. (II) When $p = 2$, an assertion corresponding to Proposition 1 is given in [4]. When $p = 3$ (resp. $p \geq 3$), an assertion similar to Proposition 1 is shown in [5] (resp. [7]) for $N = 6$ (resp. any multiple N of $p(p-1)$).

REMARK 2. This paper is the first one of the series of five papers of the same title. The other four ones II–V are already published in Proceedings of the Japan Academy, Ser. A; Vol. 77 (2001), 25–28; Vol. 77 (2001), 71–73; Vol. 77 (2001), 92–94; Vol. 78 (2002), 76–79.

2. Proof of Theorem 1

An extension of a number field is "tame" (resp. "unramified") when it is at most tamely ramified (resp. unramified) at all finite prime divisors. Let p be a fixed prime number, and ζ_p a fixed primitive p-th root of unity in the algebraic closure of $\boldsymbol{Q}$. We put $\pi = \zeta_p - 1$. Let K be a number field with $\zeta_p \in K^\times$, and E_K the group of units of K. In [2, Theorem 2.1], Gómez Ayala gave a necessary and sufficient condition for a tame Kummer extension over K of degree p to have a NIB in terms of its Kummer generator, and further, gave a generator of a NIB in an explicit form. (A similar result is also found in the unpublished paper of Kawamoto [8].) This recovers a result of Childs [1, Theorem B] on NIB of unramified Kummer extensions of degree p. The following theorem is a consequence of Theorem 2.1 of [2].

THEOREM 2. (I) *Let p, K be as above, and let a be an integer of K with $a \notin (K^\times)^p$ relatively prime to p such that $a\mathcal{O}_K$ is square free. Then, the Kummer extension $K(a^{1/p})/K$ has a NIB if and only if the integer a satisfies the congruence*

$$a \equiv \epsilon^p \mod \pi^p \tag{1}$$

for some unit $\epsilon \in E_K$.

(II) *When $p = 2$, a quadratic extension L/K has a NIB if and only if $L = K(\sqrt{a})$ for some $a \in \mathcal{O}_K$ such that $a\mathcal{O}_K$ is square free and $a \equiv 1 \bmod 4$.*

Theorem 1 follows immediately from Theorem 2 and the following:

THEOREM 3. *Let p, K and a be as in Theorem* 2 (I). *Then, the Kummer extension $K(a^{1/p})/K$ has a PIB if the integer a satisfies the congruence*

$$a \equiv u^p \mod \pi^p \tag{2}$$

for some integer $u \in \mathcal{O}_K$.

For an element $a \in K^\times$ relatively prime to p, it is well known (cf. Washington [11, Exercises 9.2, 9.3]) that the extension $K(a^{1/p})/K$ is tame (i.e., unramified at the primes over p) if and only if a satisfies the congruence (2). Theorem 3 is a generalization of a result on PIB of unramified Kummer extensions of degree p obtained independently by F. Kawamoto, N. Suwa and the author (see [6]).

Let L/K be a finite extension of degree n. We denote by $\delta(L/K)$ (resp. $d(L/K)$) the different (resp. discriminant) of L/K with respect to $\mathcal{O}_K$. For an integer γ of L, let $\delta_{L/K}(\gamma)$ (resp. $d_{L/K}(\gamma)$) be the different (resp. discriminant) of γ. For integers $\omega_1, \cdots, \omega_n$ of L, $d_{L/K}(\omega_1, \cdots, \omega_n)$ denotes the discriminant of these n integers.

Proof of Theorem 2. The assertion (II) is already known by Massy [9, Section 3]. We give a proof of the first one without using [2, Theorem 2.1] for the convenience of the reader. Let a be an integer of K with $a \notin (K^\times)^p$ relatively prime to p such that $a\mathcal{O}_K$ is square free. Let $\alpha = a^{1/p}$, $L = K(\alpha)$, $G = \mathrm{Gal}(L/K)$, and σ the generator of the cyclic group G sending α to $\zeta_p\alpha$. Here, ζ_p is the fixed primitive p-th root of unity.

First, let us assume that a satisfies the congruence (1), and show the "if" part of the assertion. It follows from (1) that $\alpha/\epsilon \equiv 1 \bmod \pi$. Then, we see that

$$\omega = \frac{1}{p}\sum_{j=0}^{p-1}\frac{\alpha^j}{\epsilon^j}$$

is an integer of L. Let X be the $p \times p$ matrix whose (i, j)-component is ζ_p^{ij}/ϵ^j with $0 \le i,\ j \le p-1$. Then, we see that

$$^t(\omega,\ \sigma(\omega), \cdots, \sigma^{p-1}(\omega)) = \frac{1}{p}X \cdot {}^t(1,\ \alpha, \cdots, \alpha^{p-1})\,, \tag{3}$$

where ${}^t(*)$ denotes the tranpose of a matrix $(*)$. The extension L/K is tame by (1) and the remark just after the statement of Theorem 3. Further, we see that $d_{L/K}(\alpha) = p^p a^{p-1}$, and that $d(L/K) = a^{p-1}\mathcal{O}_K$ because L/K is tame and the integral ideal $a\mathcal{O}_K$ is square free and because of the theorem of Dedekind on discriminants. Therefore, we see from (3) that

$$d_{L/K}(\omega,\ \sigma(\omega), \cdots, \sigma^{p-1}(\omega))\mathcal{O}_K = \frac{1}{p^{2p}}|X|^2 d_{L/K}(\alpha)\mathcal{O}_K = d(L/K)\,,$$

where $|X|$ is the determinant of X. Therefore, we obtain $\mathcal{O}_L = \mathcal{O}_K[G]\omega$.

Next, we show the "only if" part. Assume that L/K has a NIB, namely that $\mathcal{O}_L = \mathcal{O}_K[G]\omega$ for some $\omega \in \mathcal{O}_L$. We show that a satisfies the congruence (1). For $i = 0,\ 1$, let $\mathcal{O}_L^{(i)}$ be the additive group of integers x of L such that $\sigma(x) = \zeta_p^i x$. Put

$$\beta_i = \sum_{j=0}^{p-1}\zeta_p^{-ij}\sigma^j(\omega) \quad (i = 0,\ 1)\,. \tag{4}$$

We easily see that $\beta_i \in \mathcal{O}_L^{(i)}$, and that $\mathcal{O}_L^{(i)} = \mathcal{O}_K \beta_i$ from the assumption $\mathcal{O}_L = \mathcal{O}_K[G]\omega$. As $\mathcal{O}_L^{(0)} = \mathcal{O}_K$, β_0 is a unit of K. As $\alpha \in O_L^{(1)}$, we have $a^{1/p} = \alpha = \beta_1\eta$ for some integer $\eta \in \mathcal{O}_K$. However, as $a\,O_K$ is square free, η must be a unit of K. On the other hand, it follows from (4) that $\beta_1 \equiv \beta_0 \bmod \pi$. Therefore, we obtain $a = (\beta_1\eta)^p \equiv (\beta_0\eta)^p \bmod \pi^p$ with $\beta_0\eta \in E_K$. □

Proof of Theorem 3. Let K be a number field with $\zeta_p \in K^\times$, and a an integer of K with $a \notin (K^\times)^p$ relatively prime to p. Assume that $a\mathcal{O}_K$ is square free and that a satisfies the congruence (2) for some $u \in \mathcal{O}_K$. Let $\alpha,\ L,\ G,\ \sigma$ be the same as in the proof of Theorem 2. By (2), the extension L/K is tame. Then, we have $\delta(L/K) = (\alpha\mathcal{O}_L)^{p-1}$ as $a\mathcal{O}_K$ is square free. From (2), we easily see that $\alpha \equiv u \bmod \pi$. Hence, $\gamma = (\alpha - u)/\pi$ is an integer of L. We see that

$$\sigma^i(\gamma) - \gamma = \frac{\zeta_p^i - 1}{\pi}\alpha \quad (1 \le i \le p-1)\,.$$

Therefore, we obtain

$$\delta_{L/K}(\gamma)\mathcal{O}_L = (\alpha\mathcal{O}_L)^{p-1} = \delta(L/K)$$

as $(\zeta_p^i - 1)/\pi$ is a (cyclotomic) unit. Hence, it follows that $\mathcal{O}_L = \mathcal{O}_K[\gamma]$. □

REMARK 3. Let p be a prime number, and K a number field with $\zeta_p \in K^\times$. Assume that K satisfies the condition

$$(\mathcal{O}_K/\pi\mathcal{O}_K)^\times = E_K \mod \pi\,. \tag{5}$$

Then, for an integer a of K relatively prime to p such that $a\mathcal{O}_K$ is square free, the Kummer extension $L = K(a^{1/p})$ over K has a NIB if it is tame. The reason is as follows. As L/K is tame, $a \equiv u^p \bmod \pi^p$ for some $u \in \mathcal{O}_K$. By (5), we have $u \equiv \epsilon \bmod \pi$ for some unit $\epsilon \in E_K$. Therefore, $a \equiv u^p \equiv \epsilon^p \bmod \pi^p$. Hence, L/K has a NIB by Theorem 2 as $a\mathcal{O}_K$ is square free.

The condition (5) is satisfied, for example, when $K = \boldsymbol{Q}(\zeta_p)$.

3. Proofs of Propositions

In what follows, we let p be a fixed odd prime number. To show Proposition 1, we need the following lemmas.

LEMMA 1. *For any integer $n \ge 2$, there exists a totally real number field of degree n in which p remains prime.*

Proof. Though this is more or less known and is an easy exercise, we give a proof for the sake of completeness. For real numbers $a_0, \cdots, a_n$, let

$$f_{\{a_i\}}(T) = a_0T^n + a_1T^{n-1} + \cdots + a_{n-1}T + a_n \ \ (\in \boldsymbol{R}[T])\,.$$

It is easy to see that there exist $a_0, \cdots, a_n\ (\in \boldsymbol{R})$ satisfying the following $n+1$ inequalities.

$$f_{\{a_i\}}(s) \begin{cases} > 0\,, & \text{for odd integers } s \text{ with } 0 \le s \le n\,, \\ < -\dfrac{s^{n+1}-1}{s-1}p\,, & \text{for even integers } s \text{ with } 0 \le s \le n\,. \end{cases}$$

This is because the coefficient matrix $(s^{n-k})_{0\le s,k\le n}$ (with $0^0 = 1$) of these linear inequalities on a_i is nonsingular. Then, for any integers $b_0, \cdots, b_n$ ($\in \mathbf{Z}$) with $a_i \le b_i < a_i + p$, we see that $f_{\{b_i\}}(s) < 0$ (resp. > 0) for each even (resp. odd) integer s with $0 \le s \le n$, and hence $f_{\{b_i\}}(T)$ has n distinct real roots. On the other hand, there exists an irreducible polynomial of degree n over $\mathbf{Z}/p\mathbf{Z}$. Therefore, we obtain the assertion by taking suitable integers $\{b_i\}$ in the above range. □

LEMMA 2. *Let K be a number field, and let $\mathfrak{M}$, $\mathfrak{N}$ ($\neq \mathcal{O}_K$) be integral ideals of K relatively prime to each other. Put*

$$P_{\mathfrak{M},\mathfrak{N}} = \{a\mathcal{O}_K \mid a \in K^\times,\ \ a \equiv 1 \mod \mathfrak{M},\, (a,\, \mathfrak{N}) = 1,\ \ a \gg 0\}\,.$$

Here, $a \gg 0$ means that a is totally positive. Let L/K be a cyclic extension of prime degree. Assume that L/K is unramified (at all the finite prime divisors) outside $\mathfrak{M}\mathfrak{N}$ and is ramified at some prime ideals dividing $\mathfrak{N}$. Then, there exist infinitely many principal prime ideals $a\mathcal{O}_K$ in $P_{\mathfrak{M},\mathfrak{N}}$ which is of degree one and remains prime in L.

Proof. As L/K is unramified outside $\mathfrak{M}\mathfrak{N}$, the canonical homomorphism

$$P_{\mathfrak{M},\mathfrak{N}} \longrightarrow \mathrm{Gal}(L/K);\ \mathfrak{A} \to (\mathfrak{A},\ L/K)$$

is well defined. Here, $(\mathfrak{A},\ L/K)$ denotes the Frobenius automorphism for the ideal $\mathfrak{A}$. As L/K is ramified at some primes dividing $\mathfrak{N}$, the map is nontrivial. Hence, it is surjective as the degree $[L : K]$ is a prime number. Therefore, the assertion follows from the Chebotarev density theorem. □

LEMMA 3. *For an integer $n \ge 1$, there exist infinitely many CM-fields k of degree $2n$ such that* (I) *p remains prime in k and* (II) *$E_k = E_{k^+}$. Here, k^+ denotes the maximal real subfield of k, and E_k (resp. E_{k^+}) is the group of units of k (resp. k^+).*

Proof. In the following, we *fix* a totally real number field k^+ of degree n in which p remains prime. Let $\{\ell_1, \cdots, \ell_r\}$ be the set of all odd prime numbers ℓ such that $\cos(2\pi/\ell) \in k^+$. Then, $k^+(\zeta_{\ell_i}) = k^+(\sqrt{a_i})$ for some $a_i \in (k^+)^\times$. Let V_1 be the subgroup of $W = (k^+)^\times/((k^+)^\times)^2$ generated by the classes $[-1]$, $[a_i]$ $(1 \le i \le r)$, and V_2 the subgroup of W generated by all the classes containing units of k^+.

Let $a \in (k^+)^\times$ be a totally positive element such that $[-a] \notin V_1V_2$, and put $k = k^+(\sqrt{-a})$. Let us show that the CM-field k satisfies the condition (II). We have $\sqrt{-1} \notin k^\times$ as $[-a] \notin V_1$ and $[-1] \in V_1$. Assume that $\zeta_\ell \in k^\times$ for some odd prime number ℓ. Then, $k = k^+(\zeta_\ell)$ and $\cos(2\pi/\ell) \in k^+$. This implies that $[-a] \in V_1$, a contradiction. Thus, the group of roots of unity in k equals $\{\pm 1\}$. Therefore, we obtain $[E_k : E_{k^+}] \le 2$ by a theorem on units of CM-fields (cf. [11, Theorem 4.12]). Now, it follows that $E_k = E_{k^+}$ from $[-a] \notin V_2$.

Assume that n is odd. Take an imaginary quadratic field $\boldsymbol{Q}(\sqrt{-d})$ in which p remains prime, and put $k = k^+(\sqrt{-d})$. We may as well assume that $[-d] \notin V_1V_2$ so that $E_k = E_{k^+}$ by the above assertion. As n is odd, p remains prime also in k.

Next, assume that n is even. We apply Lemma 2 for the quadratic extension $k^+(\sqrt{p})/k^+$ and the ideals $\mathfrak{M} = 4\mathcal{O}_K$, $\mathfrak{N} = p\mathcal{O}_K$. Then, we see that there exist infinitely many principal prime ideals $\mathfrak{l} = a\mathcal{O}_{k^+}$ of k^+ generated by an integer a relatively prime to p such that (i) $\mathfrak{l}$ remains prime in $k^+(\sqrt{p})$ and (ii) $a \equiv 1 \bmod 4$ and a is totally positive. Let $k = k^+(\sqrt{-a})$. We may as well assume that $[-a] \notin V_1V_2$ so that $E_k = E_{k^+}$. Denote by $(*/**)$ the quadratic power residue symbol over k^+. We have $(-1/p) = 1$ since n is even and p remains prime in k^+. By (i), $(p/\mathfrak{l}) = (p/a) = -1$. Then, we see that

$$(-a/p) = (-1/p)(a/p) = (p/a) = -1$$

by (ii) and the reciprocity law for power residue symbols (cf. Hasse [3, page 59]). Hence, p remains prime also in k.

Finally, it is clear that we can obtain, by the above way, infinitely many CM-fields k satisfying the conditions of Lemma 3. □

Proof of Proposition 1. First, we deal with the case where $N = 2n(p-1)$ with $n > 1$. Let k be a CM-field of degree $2n$ satisfying the conditions (I) and (II) of Lemma 3, and let $K = k(\zeta_p)$. We see that K is also a CM-field, and that $[K : \boldsymbol{Q}] = N$ by the condition (I). By (I), the multiplicative groups $(\mathcal{O}_k/p^2\mathcal{O}_k)^\times$ and $(\mathcal{O}_{k^+}/p^2\mathcal{O}_{k^+})^\times$ are isomorphic to the additive groups

$$(\mathbf{Z}/p\mathbf{Z})^{\oplus 2n} \oplus (\mathbf{Z}/(p^{2n}-1)\mathbf{Z}) \quad \text{and} \quad (\mathbf{Z}/p\mathbf{Z})^{\oplus n} \oplus (\mathbf{Z}/(p^n-1)\mathbf{Z}),$$

respectively. Denote by ρ the complex conjugation of k. The elements $e_+ = 1 + \rho$ and $e_- = 1 - \rho$ naturally act on the multiplicative group $k^\times$. Fix an integer g of k relatively prime to p such that the class $[g] = g \bmod p^2$ in $(\mathcal{O}_k/p^2\mathcal{O}_k)^\times$ is of order $p(p^{2n}-1)$. Clearly, $g^2 = g^{e_+}g^{e_-}$. As $g^{e_+} \in (k^+)^\times$, the order of the class $[g^{e_+}]$ divides $p(p^n-1)$. Hence, we see that the order of $[g^{e_-}]$ is a multiple of $(p^n+1)/2$. Let

$$\mathfrak{C} = \frac{\{x\mathcal{O}_k \mid x \in k^\times,\ (x, p) = 1\}}{\{x\mathcal{O}_k \mid x \in k^\times,\ x \equiv 1 \bmod p^2\}}$$

be the class group of principal ideals modulo p^2, and c the class containing the ideal $(g^{e_-})^p\mathcal{O}_k$. By the Chebotarev density theorem, there exist infinitely many principal prime ideals $\mathfrak{l} = a\mathcal{O}_k$ in c :

$$\mathfrak{l} = a\mathcal{O}_k, \quad \text{and} \quad a \equiv (g^{e_-})^p \bmod p^2. \tag{6}$$

The integral ideal $\mathfrak{l}\mathcal{O}_K = a\mathcal{O}_K$ is square free at K since $\mathfrak{l} \nmid p$ and K/k is unramified outside p. Therefore, by (6) and Theorem 3, the Kummer extension $L = K(a^{1/p})/K$ has a PIB. We show that it has no NIB. Assume that it has a NIB. Then, by Theorem 2, we have $a \equiv \epsilon^p \bmod \pi^p$ for some unit $\epsilon \in E_K$. Taking the norm from K to k, $a^{p-1} \equiv \eta^p \bmod \pi^p$ with $\eta = N_{K/k}\epsilon$. By the condition (I) of Lemma 3, we have $\pi^p\mathcal{O}_K \cap O_k = p^2\mathcal{O}_k$. Therefore, we obtain from (6) and the above congruence,

$$(g^{e_-})^{2p(p-1)} = (g^{(e_-)^2})^{p(p-1)} \equiv (a^{e_-})^{p-1} \equiv (\eta^{e_-})^p \mod p^2.$$

By the condition (II) of Lemma 3, we have $\eta^{e_-} = (\eta^{e_-})^\rho = (\eta^{e_-})^{-1}$. Hence, $\eta^{e_-} = \pm 1$. Therefore, from the above congruence, we see that $(p^n+1)/2$ divides $4p(p-1)$ by considering the order of the class $[g^{e_-}]$. This implies that

$$(p^n+1)|16$$

since $(p^n+1,\ p-1)=2$ and $(p^n+1,\ p)=1$. However, this is impossible when $n>1$. Therefore, L/K can not have a NIB.

Next, we deal with the case $N=2(p-1)$. Let k be an imaginary quadratic field in which p remains prime with $k \neq \boldsymbol{Q}(\sqrt{-3}),\ \boldsymbol{Q}(\sqrt{-1})$, and let $K=k(\zeta_p)$. The group $(\mathcal{O}_k/p^2\mathcal{O}_k)^\times$ is isomorphic to the additive group $(\boldsymbol{Z}/p\boldsymbol{Z})^{\oplus 2} \oplus (\boldsymbol{Z}/(p^2-1)\boldsymbol{Z})$. Let u be an integer of k relatively prime to p such that the class $[u] \in (\mathcal{O}_k/p^2\mathcal{O}_k)^\times$ is of order $p(p^2-1)$. Using u in place of g^{e_-}, we can prove the assertion similarly to the previous case. □

To show Proposition 2, we need to show the following assertion.

PROPOSITION 3. *Let $p \geq 3$, and K a number field with $\zeta_p \in K^\times$. Let a and b be integers of K with $a,\ b \notin E_K$ relatively prime to each other satisfying the following conditions.*

(i) $a \equiv b \equiv 1 \mod p^2$.

(ii) *$a\mathcal{O}_K$ and $b\mathcal{O}_K$ are square free.*

(iii) $(b/a)_p \neq 1$, *and* $(\epsilon/a)_p = 1$ *for all units* $\epsilon \in E_K$.

Here, $(*/**)_p$ denotes the p-th power residue symbol over K. Put $L=K((ab^2)^{1/p})$. Then, the Kummer extension L/K has a NIB but no PIB.

Proof. It follows from (i) and (ii) that the extension L/K is tame and that

$$d(L/K) = (ab\mathcal{O}_K)^{p-1}. \tag{7}$$

We put $A=(ab^2)^{1/p}$ for brevity. We have $A \equiv 1 \bmod \pi$ by (i). We put

$$\omega = \frac{1}{p}\left(\sum_j{}^{*} A^j + \sum_j{}^{**} \frac{A^j}{b}\right).$$

Here (and in the following), the sum $\sum_j^*$ (resp. $\sum_j^{**}$) is taken over the integers j with $0 \leq j \leq (p-1)/2$ (resp. $(p+1)/2 \leq j < p$). We see that $p\omega$ is an integer of L, and that

$$p\omega \equiv \sum_{j=0}^{p-1} A^j \equiv 0 \mod p$$

from (i) and $A \equiv 1 \bmod \pi$. Hence, ω is an integer of L. Then, it follows that $\mathcal{O}_L = \mathcal{O}_K[\mathrm{Gal}(L/K)]\omega$ immediately from (ii) and [2, Theorem 2.1]. In particular, we see that any integer γ of L can be written in the form

$$\gamma = x_0 + \sum_j{}^{*} x_j A^j + \sum_j{}^{**} x_j \frac{A^j}{b} \tag{8}$$

with $x_j \in \mathcal{O}_K[1/p]$. To show that L/K has no PIB, assume that $\mathcal{O}_L = \mathcal{O}_K[\gamma]$ for some $\gamma \in \mathcal{O}_L$. Let σ be the generator of $\mathrm{Gal}(L/K)$ sending A to $\zeta_p A$. From (8), we see that $\sigma^j(\gamma) - \gamma$ is divisible by any prime ideal $\mathfrak{P}$ of L dividing ab $(1 \leq j < p)$. This implies that

$$(\sigma(\gamma) - \gamma)\mathcal{O}_L = \prod_{\mathfrak{P}|ab} \mathfrak{P}$$

by (7) and the assumption $\mathcal{O}_L = \mathcal{O}_K[\gamma]$, where $\mathfrak{P}$ runs over the primes of L dividing ab. Hence, by the condition (ii), we obtain

$$N_{L/K}(\sigma(\gamma) - \gamma) = ab\epsilon \tag{9}$$

for some unit $\epsilon \in E_K$. Here, $N_{L/K}$ is the norm map. Let $\mathfrak{L}$ be a prime ideal of L dividing a. From (8), we see that

$$\sigma(\gamma) - \gamma \equiv \pi x_1 (ab^2)^{1/p} \mod \mathfrak{L}^2.$$

Therefore,

$$\frac{\pi x_1 (ab^2)^{1/p}}{\sigma(\gamma) - \gamma} \equiv 1 \mod \prod_{\mathfrak{L}|a} \mathfrak{L}.$$

Here, $\mathfrak{L}$ runs over the prime ideals of L dividing a. Then, taking the norm, we obtain

$$\pi^p x_1^p b \equiv \epsilon \mod a\mathcal{O}_K$$

by (9) and the condition (ii). However, this congruence can not hold by the condition (iii). Therefore, L/K has no PIB. □

Proof of Proposition 2. Let K be a number field with $\zeta_p \in K^\times$. We easily see that there exist infinitely many principal prime ideals $b\mathcal{O}_K$ of K with $b \equiv 1 \bmod p^2$. We fix one of such prime ideals $b\mathcal{O}_K$. Put

$$K' = K(\epsilon^{1/p} | \epsilon \in E_K) \quad \text{and} \quad K'' = K'(b^{1/p}).$$

Applying Lemma 2 for the extension K''/K' of degree p and the ideals $\mathfrak{M} = p^2\mathcal{O}_{K'}$, $\mathfrak{N} = b\mathcal{O}_{K'}$, we see that there exist infinitely many principal prime ideals $\alpha\mathcal{O}_{K'}$ $(\in P_{\mathfrak{M},\mathfrak{N}})$ of degree one which remain prime in K''. Here, $P_{\mathfrak{M},\mathfrak{N}}$ is the group of principal ideals defined in Lemma 2. Let $a = N_{K'/K}\alpha$. Then, $a\mathcal{O}_K$ is a prime ideal of K which splits completely in K' and remains prime in $K(b^{1/p})$. Now, it follows that the couple (a, b) satisfies the conditions in Proposition 3. From this, we obtain Proposition 2. □

ACKNOWLEDGEMENTS. The author was partially supported by Grant-in-Aid for Scientific Research (C), (No. 13640036), the Ministry of Education, Culture, Sports, Science and Technology of Japan.

References

[1] L. Childs, The group of unramified Kummer extensions of prime degree, Proc. London Math. Soc., **35** (1977), 407–422.
[2] E. J. Gómez Ayala, Bases normales d'entiers dans les extensions de Kummer de degré premier, J. Théor. Nombres Bordeaux, **6** (1994), 95–116.
[3] H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil II, Physica-Verlag, Würzburg-Wien, 1965.
[4] H. Ichimura, A note on unramified quadratic extensions over algebraic number fields, Proc. Japan Acad., **76A** (2000), 78–81.
[5] H. Ichimura, A note on integral bases of unramified cyclic extensions of prime degree, Abh. Math. Univ. Hamburg, **70** (2000), 275–279.
[6] H. Ichimura, On power integral bases of unramified cyclic extensions of prime degree, J. Algebra, **235** (2001), 104–112.
[7] H. Ichimura and H. Sumida, A note on integral bases of unramified cyclic extensions of prime degree, II, Manuscripta Math., **104** (2001), 201–210.
[8] F. Kawamoto, Normal Integral Bases and Divisor Polynomials. Thesis, Gakushuin Univ., 1986.
[9] R. Massy, Bases normales d'entiers relatives quadratiques, J. Number Theory, **38** (1991), 216–239.
[10] A. Srivastav and S. Venkataraman, Relative Galois module structure of quadratic extensions, Indian J. Pure Appl. Math., **25** (1994), 473–488.
[11] L. Washington, Introduction to Cyclotomic Fields (2-nd edition), Springer-Verlag, New York 1996.

Humio Ichimura
Department of Mathematics
Yokohama City University
22–2, Seto, Kanazawa-ku
Yokohama 236–0027
Japan
e-mail: ichimura@yokohama-cu.ac.jp